

## **REMARKS**

This communication is in response to the Office Action mailed March 30, 2006. The Examiner now relies on the newly-cited Klug patent (5,790,785) as an anticipatory reference and, for some claims, as a primary reference of an obviousness rejection. No claims have been amended in this response. Applicant respectfully traverses the rejections.

Applicant's claim 1 includes "generating a user registration page request . . . and forwarding the user registration page request to the application server." Claim 1 further recites "by the application server, embedding security registration data requirements in the user registration page request and forwarding the user registration page request to a user registration page of the web application."

Klug discloses, using the terminology used in the claims (assuming such terminology could even properly be applicable to Klug, as the Examiner appears to be applying Klug to the claims), an "application server" that operates as a "registrar web site" so that users do not have to register with individual third party web sites. See, e.g., the Klug Abstract and Fig. 1. That is, in lieu of a user registering with an individual third party web site, the user instead provides, to the third party web site, the user id and password of the registrar web site. The third party web site, in turn, obtains the appropriate registration data, corresponding to the user id and password, from the registrar web site.

On the other hand, the subject matter of Applicant's claim 1 involves interoperation between an application server and a web application to cause the request, from a user, not only user profile registration requirements of the web application but, also, security registration data requirements of the application server. In particular, claim 1 recites "by the application server, embedding security registration data requirements in the user registration page request and forwarding the user registration page request to a user registration page of the web application." Klug does not disclose such an "embedding" step. Klug's disclosure of "a registrar application 128 outputs a request to the user to select a user ID and password" is not the same as "embedding" the security registration data requirements in the user registration page request. (Note that the user registration page request is not the user registration page itself.)

In addition, claim 1 further recites "by the user registration page of the web application, merging the security registration data requirements from the application server with user profile registration requirements of the web application to form a user information request page." It is

this merged user information request page that is used to form the user information request page, that is sent from the web application to the user, for the user to fill out. Klug does not appear to disclose such a “merging” step. The Examiner’s citation of col. 7, lines 26-45, certainly does not appear to disclose such a merging.

From the filled-out user information request page, the application server extracts “security data from the filled out user information request page.” Klug does not disclose such an “extracting” step.

The application server bootstraps a user account, for the web application, based upon the extracted security data. The “security registration data requirements” recited in claim 1 may include, for example, “username, password, realm , etc” (see page 10, line 20, of Applicant’s specification). Klug does not disclose using security data extracted from a user information (where the user information page results from merging user registration data requirements with security registration data requirements provided by an application data server) for an application server to bootstrap a user account.

The “security registration data requirements” are indications to require security registration data, and are not security registration data themselves. For example, the security registration data requirements provided from the application server to the web application may be requirements for a user to provide a user id and password. That is, the user registration page provided to the user by the web application will, as a result, require the user to enter a user id and password (which can then be extracted for use by the application server, to bootstrap a user account).

In summary, in claim 1, security registration data requirements are provided from the application server to the web application. In Klug, the username and password (even assuming these are requirements for security registration data, which they are not) are never embedded into a user registration page request.

If the Examiner continues to contend that Klug discloses such a feature, Applicant respectfully requests the Examiner to particularly point out which specific step of, for example, the cited Fig. 2B flowchart, discloses this feature. In addition, if the Examiner could more particularly support the contention (e.g., by citing to particular elements of the disclosure, by reference numeral), this would greatly help Applicant to understand and more particularly respond to the Examiner’s contention.

The remaining independent claims are analogous to claim 1 and, therefore, the discussion above relative to claim 1 is equally applicable to those remaining independent claims.

With regard to Levergood, the Examiner states that

Levergood substantially teaches that “the authentication server checks to see if the user qualifies for a new account” (see column 6, line 67 –column 7, line 3), meeting the limitation of making available a set of user security requirements.

As discussed above relative to Klug, claim 1 recites that the “security registration data requirements” are provided to the web application by the application server, by embedding the security registration data requirements into the user registration page request. In addition, the user profile registration data is provided from the user, via the user registration page (into which the security registration data requirements are merged). Levergood’s alleged disclosure of the authentication sever checking to see if the user qualifies for a new account does not suggest modifying Klug such that the security registration data requirements are embedded in a user registration page request.

### **CONCLUSION**

Applicant has thus shown that, first, Klug does not anticipate the subject matter of the independent claims since, for example, the Klug registrar web site does not embed security registration data requirements into a user registration page request. Furthermore, Levergood does not suggest such a feature, either.

Applicant believes that all pending claims are allowable and respectfully requests a Notice of Allowance for this application from the Examiner. Should the Examiner believe that a telephone conference would expedite the prosecution of this application, the undersigned can be reached at the telephone number set out below.

Respectfully submitted,  
BEYER WEAVER & THOMAS, LLP

/ASH/  
Alan S. Hodes  
Reg. No. 38,185

P.O. Box 70250  
Oakland, CA 94612-0250  
(650) 961-8300